DATE(S) ISSUED:
12/14/2011

SUBJECT:
Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (MS11-094)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft PowerPoint, a program used for creating presentations. These vulnerabilities can be exploited by opening a specially crafted PowerPoint file received as an email attachment, by visiting a web site that is hosting a specially crafted PowerPoint file, or by opening a legitimate PowerPoint file that is located in the same network directory as a specially crafted library file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
·   Microsoft Office 2008 for Mac
·   Microsoft Office 2007
·   Microsoft Office 2010
·   Microsoft PowerPoint Viewer 2007
·   Microsoft Office Compatibility Pack for Word, Excel, and
    PowerPoint 2007 File Formats

RISK:
Government:
·   Large and medium government entities: **High**
·   Small government entities: **High**

Businesses:
·   Large and medium business entities: **High**
·   Small business entities: **High**

Home users: High

DESCRIPTION:
Two remote code execution vulnerabilities have been discovered in Microsoft PowerPoint. The first vulnerability is caused by the way Microsoft PowerPoint improperly restricts the path used for loading external libraries. This issue could be exploited if an attacker placed a specially crafted DLL on a network share and then convinced a user to open a PowerPoint file also contained in the same network directory.

The second vulnerability is a memory corruption issue derived from the way Microsoft PowerPoint improperly reads an invalid record a PowerPoint file. As a result, PowerPoint may cause memory corruptions that could allow an attacker to execute remote code. This vulnerability can be exploited via an email attachment or through the Web. In an email-based scenario, the user would have to open the specially crafted PowerPoint presentation as an email attachment. In a Web based scenario, a user would visit a website and then open the specially crafted PowerPoint presentation that is hosted on the page.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider installing Microsoft's Office File Validation tool for Microsoft PowerPoint 2003 and PowerPoint 2007 (http://www.microsoft.com/technet/security/advisory/2501584.mspx)   which would prompt the user for files that fail the Office File Validation and a user would have to click through the warning messages to open them before any of these vulnerabilities are exploited.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Remind users not to open e-mail attachments from unknown or untrusted sources.

REFERENCES:
Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms11-094

Security Focus:
http://www.securityfocus.com/bid/50964
http://www.securityfocus.com/bid/50967

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3396
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3413